

30097



19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

12 Offenlegungsschrift
10 DE 196 23 145 A 1

51 Int. Cl.⁶:
G 11 C 7/00
G 11 C 16/06
B 60 K 28/00

21 Aktenzeichen: 196 23 145.0
22 Anmeldetag: 10. 6. 96
43 Offenlegungstag: 11. 12. 97

ZGM/ZGE
10. DEZ 1997
Eingang

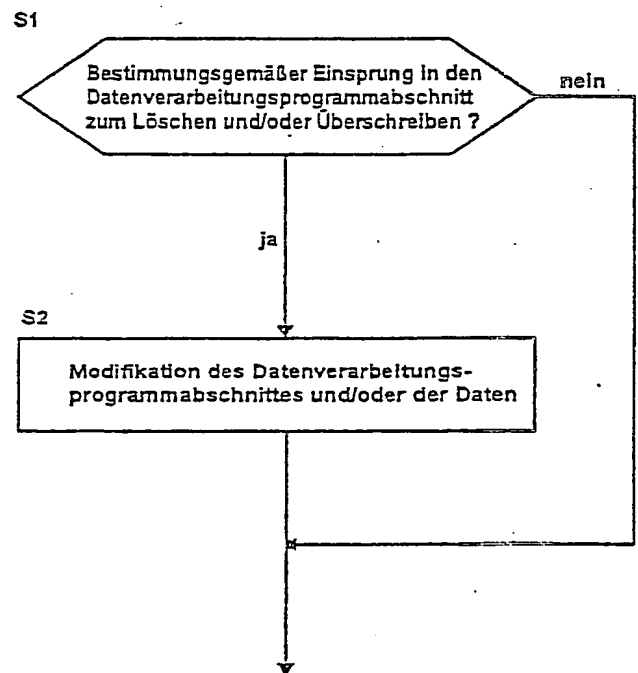
DE 196 23 145 A 1

71 Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

72 Erfinder:
Werner, Andreas, 73262 Reichenbach, DE; Franz,
Carsten, 71706 Markgröningen, DE; Schulz, Udo,
71665 Vaihingen, DE; Nagl, Walter, Wilfersdorf, DE

54 Verfahren zum Betreiben eines Steuergerätes mit einer über eine Programmiervorrichtung programmierbaren Speichereinrichtung

57 Es wird ein Verfahren zum Betreiben eines Steuergerätes (10) mit einer über eine Programmiervorrichtung (20) programmierbaren Speichereinrichtung (14) beschrieben, wobei das Löschen und das Überschreiben des Inhalts der Speichereinrichtung jeweils unter Ausführung eines Datenverarbeitungsprogrammabschnittes und unter Verwendung von Daten durchgeführt wird. Das beschriebene Verfahren zeichnet sich dadurch aus, daß wenigstens entweder der Datenverarbeitungsprogrammabschnitt oder die Daten dertart bereitgestellt werden, daß sie vor deren Verwendbarkeit zur Herbeiführung eines Löschens oder eines Überschreibens einer Modifikation bedürfen, und daß diese Modifikation erst durchgeführt wird, wenn festgestellt wird, daß ein Einsprung in den Datenverarbeitungsprogrammabschnitt bestimmungsgemäß erfolgt ist oder erfolgen wird oder erfolgen kann.



DE 196 23 145 A 1

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren gemäß dem Oberbegriff des Patentanspruchs 1, d. h. ein Verfahren zum Betreiben eines Steuergerätes mit einer über eine Programmervorrichtung programmierbaren Speichereinrichtung, wobei das Löschen und das Überschreiben des Inhalts der Speichereinrichtung jeweils unter Ausführung eines Datenverarbeitungsprogrammabschnittes und unter Verwendung von Daten durchgeführt wird.

Ein derartiges Verfahren ist beispielsweise in der DE 43 32 499 A1 offenbart. Das in dieser Druckschrift beschriebene Steuergerät ist ein Kraftfahrzeugsteuergerät, dessen möglicher Aufbau und Einbettung in ein Gesamtsystem nachfolgend unter Bezugnahme auf Fig. 3 näher beschrieben wird.

Das Kraftfahrzeugsteuergerät ist in der Fig. 3 mit dem Bezugszeichen 10 bezeichnet; es enthält einen Mikrorechner 11 und Ein-/Ausgabeschaltkreise 12.

Der Mikrorechner 11 umfaßt eine Zentraleinheit 13, einen elektrisch löscht- und programmierbaren Speicher 14 in Form eines Flash-EPROM, einen Schreib-/Lesespeicher 15, einen Nur-Lese-Speicher 16 und eine serielle Schnittstelle 21.

Das Kraftfahrzeugsteuergerät 10 erhält über die Ein-/Ausgabeschaltkreise 12 Eingangssignale von Sensoren wie einem Drosselklappenpotentiometer 17, einem Drehzahlfühler 23 und weiteren Sensoren 18. Die weiteren Sensoren, auf welche hier nicht näher eingegangen werden soll, sind je nach Kraftfahrzeugsteuergerät ein Motor-Temperaturfühler, ein Ansaugluft-Temperaturfühler, ein Luftmassenmesser, ein Leerlaufschalter usw.

Das Kraftfahrzeugsteuergerät 10 gibt andererseits über die Ein-/Ausgabeschaltkreise 12 Ausgangssignale an Aktuatoren 19 zur Steuerung von beispielsweise Einspritzventilen, Zündspulen usw. aus.

Der genaue Aufbau des Kraftfahrzeugsteuergerätes 10 kann der Druckschrift Bosch — Technische Unter- richtung, kombiniertes Zünd- und Benzineinspritzsystem Motronic, Robert Bosch GmbH, 1983 entnommen werden und bedarf hier deshalb keiner näheren Erläute- rung.

Die genannten Speichereinrichtungen 14, 15 und 16 sind der Zentraleinheit 13 zugeordnet und dienen zur Speicherung von Programmen und Daten für die Zentraleinheit 13.

Die Verwendung von elektrisch löscht- und programmierbaren nichtflüchtigen Speichereinrichtungen wie der Speichereinrichtung 14 erweist sich bei einem Kraftfahrzeugsteuergerät als vorteilhaft, weil diese sich jederzeit umprogrammieren lassen, was insbesondere bei später entdeckten Fehlern oder individuellen Kundenwünschen von nicht unerheblicher Bedeutung ist.

Die Verwendung von Flash-EPROMs als elektrisch löscht- und programmierbare nichtflüchtige Speicher- einrichtungen gewinnt dabei zunehmend an Bedeutung, weil diese die Vorzüge eines "normalen" EPROM (hohe Speicherzellendichte) und eines EEPROM (elektrisches und damit einfaches und bequemes Löschen des Spei- cherinhalts) in sich vereinen.

Zur anfänglichen Programmierung der Flash- EPROMs (vorzugsweise in Abhängigkeit vom Kraft- fahrzeug-Typ im Kraftfahrzeug-Herstellungsbetrieb) oder zur späteren Umprogrammierung derselben (beim Kundendienst zur Fehlerbeseitigung oder entsprechend individuellen Kundenwünschen) wird ein externes Pro- grammiergerät 20, beispielsweise in Form eines Perso-

nal Computer an das Steuergerät 10 angeschlossen.

Der Anschluß erfolgt beispielsweise über eine serielle Schnittstellenleitung 22 und die bereits erwähnte serielle Schnittstelle 21.

Durch das externe Programmiergerät 20 ist das Steu- ergerät 10 bei Bedarf zur Ausführung von Datenverar- beitungsprogrammabschnitten zum Löschen bzw. Überschreiben von Daten im Flash-EPROM veranlaß- bar, wobei gegebenenfalls auch die (neu) einzuspei- chernden Daten zur Verfügung gestellt werden.

Das Steuergerät 10 selbst kann die Ausführung der genannten Datenverarbeitungsprogrammabschnitte im Normalfall nicht von sich aus, also nicht ohne externen Anstoß veranlassen. D.h., in den während des Fahrbe- triebes im Steuergerät ausgeführten oder auszuführen- den Anwenderprogrammen ist kein Einsprung in die genannten Datenverarbeitungsprogrammabschnitte vorgesehen. Der Grund für diese Maßnahme liegt unter anderem darin, daß ein unbeabsichtigtes oder ein unbe- fugtes Löschen und/oder Überschreiben des Flash- EPROM verhindert werden soll.

Eine weitere Maßnahme zum Schutz vor unbeabsich- tigten Speicherinhaltsveränderungen und vor Manipu- lationen durch hierzu nicht Berechtigte besteht dar- in, daß dem eigentlichen Löschen und/oder Überschreiben von Inhalten des Flash-EPROM eine Berechtigungs- kontrolle (durch Überprüfen eines eingegebenen Paß- wortes oder dergleichen) vorausgeht.

Durch die genannten Schutzvorkehrungen sind ein unbeabsichtigtes oder unbefugtes Löschen und/oder Überschreiben des Flash-EPROM weitestgehend ver- hinderbar. Allerdings ist es bei einer unglücklichen Ver- kettung gewisser Umstände nicht vollständig aus- schließbar, daß diese Schutzmaßnahmen vereinzelt nicht wirksam sind.

Verantwortlich hierfür sind vor allem EMV-Einstrah- lungen ins Steuergerät, aber auch gezielte Manipulation- en des Adreßzeigers oder des Adreßbusses durch un- befugte Dritte.

Die Folge hiervon ist, daß — obgleich dies nicht vor- gesehen ist — unter ungünstigen Bedingungen zumin- dest theoretisch auch ohne bestimmungsgemäße Veran- lassung durch das Programmiergerät ein Einsprung in einen Datenverarbeitungsprogrammabschnitt erfolger- kann, durch dessen Ausführung im Flash-EPROM d. Steuergerätes gespeicherte Daten gelöscht und/oder überschrieben werden können.

Sofern ein Einsprung an den Anfang einer derartigen Routine erfolgt, kann ein drohender Schaden durch Ab- frage eines Paßwortes oder dergleichen und gegeb- enfalls Verlassen der Routine abgewendet werden. Falls der Einsprung jedoch an eine Stelle weiter hinten im Programm erfolgt, ist dieser Schutzmechanismus un- wirksam, so daß ein nicht bestimmungsgemäßes Lö- schen und/oder Überschreiben von in einer program- mierbaren Speichereinrichtung gespeicherten Daten hierdurch nicht zuverlässig ausgeschlossen werden kann.

Zur Abhilfe hiergegen sind an den Flash-EPROMs zum Teil Programmierspannungseingänge vorgesehen, an welche eine vorbestimmte Programmierspannung anzulegen ist, wenn ein Löschen oder Beschreiben der Speichereinrichtung durchgeführt werden soll. Ein der- artiger Schutzmechanismus erfordert jedoch einen zu- sätzlichen Hardwareaufwand, der aufgrund der Tatsa- che, daß die vorbestimmte Programmierspannung rela- tiv genau eingehalten werden muß, nicht unerhebliche Ausmaße annehmen kann, was seinerseits wiederum

auch negative Auswirkungen auf die Zuverlässigkeit bzw. Fehleranfälligkeit des Schutzmechanismus selbst haben kann.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde, das Verfahren gemäß dem Oberbegriff des Patentanspruchs 1 derart weiterzubilden, daß ein nicht bestimmungsgemäßes Löschen und/oder Überschreiben von in einer programmierbaren Speichereinrichtung gespeicherten Daten auf einfache Weise zuverlässig ausschließbar ist.

Diese Aufgabe wird erfindungsgemäß durch die im kennzeichnenden Teil des Patentanspruchs 1 beanspruchten Merkmale gelöst.

Demnach ist vorgesehen, daß wenigstens entweder der Datenverarbeitungsprogrammabschnitt oder die (vom Datenverarbeitungsprogrammabschnitt verwendeten) Daten derart bereitgestellt werden, daß sie vor deren Verwendbarkeit zur Herbeiführung eines Lösches oder eines Überschreibens einer Modifikation bedürfen, und daß diese Modifikation erst durchgeführt wird, wenn festgestellt wird, daß ein Einsprung in den Datenverarbeitungsprogrammabschnitt bestimmungsgemäß erfolgt ist oder erfolgen wird oder erfolgen kann.

Ein Einsprung in einen Datenverarbeitungsprogrammabschnitt zum Löschen und/oder Überschreiben des Inhalts der programmierbaren Speichervorrichtung kann mithin nur dann zu einem Löschen und/oder Überschreiben führen, wenn aufgrund der Begleitumstände zumindest mit hoher Wahrscheinlichkeit davon ausgegangen werden kann oder konnte, daß die Löschen- und/oder Überschreibroutine nicht versehentlich oder mißbräuchlich aufgerufen wurde, wird oder werden wird.

Die Durchführung einer derartigen Überprüfung und der in Abhängigkeit hiervon erforderlichen Code- und/oder Datenmodifikation ist relativ einfach durchführbar. Bei geeigneter Auswahl der Umstände, anhand derer festgestellt wird, ob ein Einsprung in den Datenverarbeitungsprogrammabschnitt bestimmungsgemäß erfolgt ist oder erfolgen wird oder erfolgen kann (beispielsweise bei einer Entscheidung in Abhängigkeit davon, ob ein externes Programmiergerät oder dergleichen angeschlossen und/oder aktiviert ist), ist der erfindungsgemäße Schutzmechanismus auch äußerst zuverlässig, also kaum zu umgehen.

Es wurde mithin ein Verfahren geschaffen, durch welches ein nicht bestimmungsgemäßes Löschen und/oder Überschreiben von in einer programmierbaren Speichereinrichtung gespeicherten Daten auf einfache Weise zuverlässig ausschließbar ist.

Der Ausschluß des nicht bestimmungsgemäßen Lösches sichert nicht nur die gespeicherten Daten vor einer ungewollten oder unbefugten Veränderung, sondern trägt auch erheblich zur Betriebssicherheit des Steuergerätes bei, denn ein Sprung aus einem während des Fahrbetriebs ausgeführten Anwenderprogramm in einen Datenverarbeitungsprogrammabschnitt zum Löschen und/oder Überschreiben des Flash-EPROM könnte insbesondere bei einem zu diesem Zeitpunkt fahrenden Kraftfahrzeug erhebliche Sicherheitsrisiken mit sich bringen.

Vorteilhafte Weiterbildungen der Erfindung sind Gegenstand der Unteransprüche.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels näher erläutert. Es zeigen

Fig. 1 einen prinzipiellen Ablaufplan des erfindungsgemäßen Verfahrensabschnittes,

Fig. 2A bis 2D Ablaufpläne, die ein bestimmungsgemäßes Löschen eines Flash-EPROM veranschaulichen,

und

Fig. 3 eine Anordnung, die ein vor einem nicht bestimmungsgemäßes Löschen und/oder Überschreiben zu schützendes Flash-EPROM enthält.

Die nachstehenden Erläuterungen beziehen sich auf ein Verfahren zum Betreiben eines Steuergerätes zur Steuerung beispielsweise des Motors, des Getriebes der Bremsen etc. eines Kraftfahrzeuges, also eines Kraftfahrzeugsteuergerätes.

Das betrachtete Kraftfahrzeugsteuergerät enthält programmierbare Speichereinrichtungen, genauer gesagt elektrisch löschen- und programmierbare (nichtflüchtige) Speichereinrichtungen in Form von Flash-EPROMs. Die Programmierung dieser Flash-EPROMs erfolgt über ein externes Programmiergerät, das beispielsweise über eine serielle Schnittstelle mit dem Kraftfahrzeugsteuergerät verbindbar ist.

Eine mögliche Ausführungsform einer ein derartiges Kraftfahrzeugsteuergerät enthaltenden Anordnung ist die in der Fig. 3 gezeigte Anordnung, auf deren eingangs bereits erfolgte ausführliche Beschreibung hiermit ausdrücklich Bezug genommen wird.

Die vorliegende Erfindung ist jedoch nicht auf die Programmierung von Flash-EPROMs in Kraftfahrzeugsteuergeräten unter Verwendung eines externen Programmiergerätes beschränkt. Sie ist vielmehr überall dort anwendbar, wo es ganz allgemein darum geht, eine Speichereinrichtung eines Steuergerätes durch eine Programmiervorrichtung zu programmieren.

Das Programmieren, genauer gesagt das Löschen und das Überschreiben des Inhalts des Flash-EPROMs wird jeweils unter Ausführung eines Datenverarbeitungsprogrammabschnittes im Steuergerät und unter Verwendung von (für die ordnungsgemäße Ausführung des Datenverarbeitungsprogrammabschnittes benötigten) Daten durchgeführt.

Die jeweiligen Datenverarbeitungsprogrammabschnitte sind gemäß einem ersten Aspekt der Erfindung jedoch nicht einfach durch einen Aufruf oder einen Einsprung in dieselben ausführbar, sondern liegen vorteilhafter Weise zunächst in einer Form vor, in der ein Löschen und/oder ein Überschreiben von Daten im Flash-EPROM noch nicht bewerkstelligbar ist.

Diese Nicht-Ausführbarkeit kann auf verschiedenste Art und Weise erreicht werden.

Eine der Möglichkeiten hierfür besteht darin, daß der die jeweiligen Datenverarbeitungsprogrammabschnitte repräsentierende Code zumindest teilweise derart verschlüsselt oder in sonstiger Weise manipuliert ist, daß er ohne eine entsprechende Modifikation ein zumindest nicht vollständig und/oder nicht ordnungsgemäß ausführbares Programm darstellt.

Eine weitere Möglichkeit besteht darin, daß in den Code an strategisch günstigen Stellen Befehle eingebaut sind, durch die die Ausführung von Befehlen, welche letztlich das Löschen und/oder Überschreiben von Daten im Flash-EPROM bewirken sollen, unterbunden wird. Dies können beispielsweise Sprunganweisungen sein, die ein Verlassen des betreffenden Datenverarbeitungsprogrammabschnittes oder ein Überspringen der kritischen Anweisungen bewirken, und die vor einer ordnungsgemäßen Programmausführung durch eine entsprechende Modifikation des Programmcodes zu entfernen oder wenigstens unwirksam zu machen sind.

Gemäß einem zweiten Aspekt der Erfindung können alternativ oder zusätzlich hierzu Daten, von deren Inhalt das Löschen und/oder Überschreiben des Inhalts des Flash-EPROMs abhängig machbar ist, auf (nicht

plausible) Werte gesetzt sein, die das Löschen und/oder Überschreiben des Flash-EPROM verhindern.

Bei den genannten Daten kann es sich beispielsweise um diejenigen Daten und Adressenwerte handeln, die zumindest bei einigen Flash-EPROMs vor dem eigentlichen Löschen und/oder Überschreiben in Form sogenannter Entriegelungszyklen (unlock cycles) über den Bus zum Flash-EPROM gegeben werden müssen. Während der besagten unlock cycles müssen bestimmte Daten in einer bestimmten Reihenfolge an bestimmte Adressen des Flash-EPROM geschrieben werden, um das Flash-EPROM zum Zwecke des Datenlöschens und/oder -überschreibens aufzusperren bzw. zu entriegeln. Scheitert der Versuch, das Flash-EPROM zu entriegeln, so bleibt es für ein Löschen und/oder Überschreiben gesperrt.

Sorgt man nun dafür, daß durch die in den unlock cycles ausgegebenen Adressen und Daten nicht automatisch, sondern nur unter ganz bestimmten Umständen, nämlich nur bei bestimmungsgemäß veranlaßtem Löschen und/oder Überschreiben des Flash-EPROM eine Entriegelung des Flash-EPROM bewirkbar ist, so steht ein weiterer Schutzmechanismus zur Verfügung, durch welchen ein nicht bestimmungsgemäßes Löschen und/oder Überschreiben des Flash-EPROM verhindert ist.

Zur Vermeidung der automatischen Entriegelbarkeit des Flash-EPROM kann vorgesehen werden, daß der Datenverarbeitungsprogrammabschnitt die während der unlock cycles zum Flash-EPROM auszugebenden Daten und/oder Adressen nicht wie bisher üblich im Programmcode integriert hat, sondern aus einem vorzugsweise flüchtigen Speicher (RAM) holen muß, wobei der Speicherbereich (die Variablen-tabelle), aus dem sich die jeweiligen Datenverarbeitungsprogrammabschnitte die Daten und/oder Adressen zur Ausgabe der unlock cycles holen, nicht automatisch mit Werten beschrieben ist, deren Verwendung das Flash-EPROM entriegelt.

In einer praktischen Realisierung dieses Schutzmechanismus kann vorgesehen werden, die eine Entriegelung des Flash-EPROM ermöglichenden Daten erst dann in die genannte Variablen-tabelle einzuschreiben, wenn feststeht, daß eine bestimmungsgemäß zustande gekommene (beispielsweise durch das Programmiergerät veranlaßte) Anforderung zum Löschen oder überschreiben des Flash-EPROM vorliegt oder folgen wird oder folgen kann, und daß die genannten Daten in der Variablen-tabelle unmittelbar nach dem Löschen bzw. Überschreibvorgang im Flash-EPROM wieder gelöscht oder durch eine Entriegelung des Flash-EPROM ausschließende Daten ersetzt werden. Ein Löschen der Daten in der Variablen-tabelle bzw. ein überschreiben derselben durch eine Entriegelung des Flash-EPROM ausschließende Daten ist unter anderem auch nach dem Einschalten oder nach einem Rücksetzen des Steuergerätes angezeigt, um eine zufällige Entriegelbarkeit des Flash-EPROM zuverlässig verhindern zu können.

Bei Vorsehen von Schutzmechanismen gemäß dem ersten und/oder zweiten Aspekt der vorliegenden Erfindung, d. h. bei Vorsehen von die ordnungsgemäße Ausführbarkeit der jeweiligen Datenverarbeitungsprogrammabschnitte zum Löschen und/oder Überschreiben des Flash-EPROM Einfluß nehmenden Schutzmechanismen hat ein Einsprung in die entsprechenden Datenverarbeitungsprogrammabschnitte nicht automatisch ein Löschen und/oder Überschreiben von Daten im Flash-EPROM zur Folge. Vielmehr ist auf diese Weise ein Löschen und/oder Überschreiben von Daten im

Flash-EPROM grundsätzlich zunächst einmal ausgeschlossen.

Falls ein bestimmungsgemäßes Löschen und/oder Überschreiben von Daten im Flash-EPROM durchgeführt werden soll, bedarf es, wie bereits angedeutet wurde, einer Modifikation des jeweiligen Datenverarbeitungsprogrammabschnittes und/oder der die Daten für die unlock cycles enthaltenden Variablen-tabelle im Steuergerät.

Dieser Vorgang ist in der Fig. 1 veranschaulicht.

Gemäß der Darstellung in der Fig. 1 wird in einem ersten Schritt S1 zunächst überprüft, ob ein Einsprung in einen Datenverarbeitungsprogrammabschnitt zum Löschen und/oder Überschreiben von Daten eines Flash-EPROM bestimmungsgemäß, d. h. zumindest nicht offensichtlich versehentlich oder mißbräuchlich erfolgt ist, erfolgen wird oder erfolgen kann. Die Überprüfung konzentriert sich dabei vorzugsweise auf solche Kriterien, deren Vorliegen allein oder in Kombination mit anderen Bedingungen das Einleiten einer Programmierung des Flash-EPROM nicht nur möglich erscheinen lassen (nicht ausschließen), sondern aus denen sich auch mit einer gewissen Zuverlässigkeit folgern läßt, daß die Programmierung des Flash-EPROM tatsächlich eingeleitet bzw. veranlaßt wurde oder werden wird.

Für den Fall, daß zur Programmierung des Flash-EPROM wie im vorliegenden Ausführungsbeispiel ein externes Programmier- oder Testgerät an das Steuergerät angeschlossen werden muß, kann im Feststellungsschritt S1 unter anderem beispielsweise überprüft werden,

- ob ein entsprechendes externes Programmiergerät angeschlossen ist, und/oder
- ob das Programmiergerät aktiviert (eingeschaltet) ist, und/oder
- ob sich das Programmiergerät in einer Programmierbetriebsart befindet, und/oder
- ob eine bestimmungsgemäße Kommunikation zwischen Steuergerät und Programmiergerät stattfindet oder stattgefunden hat.

Die Durchführung einer oder mehrerer der genannten oder ähnlicher Überprüfungen ermöglicht eine sehr sichere Aussage darüber, ob ein Einsprung in die Programmerroutine zum Programmieren des Flash-EPROM bestimmungsgemäß veranlaßt wurde oder veranlaßt werden wird.

Die in diesem Zusammenhang im einzelnen durchzuführenden Überprüfungen hängen von den jeweiligen individuellen Gegebenheiten ab. Denkbar wären in diesem Zusammenhang insbesondere (aber nicht ausschließlich) Abfragen von entsprechenden Statusinformationen des Steuergerätes und gegebenenfalls von daran angeschlossenen externen Geräten und/oder die Abfrage von Kennungen, die bei Eintreten gewisser Ereignisse gesetzt werden.

Wird bei der Überprüfung in Schritt S1 festgestellt, daß ein bestimmungsgemäßer Einsprung in den Datenverarbeitungsabschnitt zum Löschen und/oder Überschreiben des Flash-EPROM momentan und/oder in absehbarer Zeit danach nicht vorliegt oder nicht vorliegen kann, wird der in der Fig. 1 gezeigte Programmabschnitt unter Auslassung des nachfolgend noch näher beschriebenen Schrittes S2 verlassen. Das Auslassen des Schrittes S2 bewirkt, daß ein gegebenenfalls erfolgter oder erfolgreicher Einsprung in einen Datenverarbeitungsprogrammabschnitt zum Löschen und/oder Über-

schreiben eines Flash-EPROM kein Löschen und/oder Überschreiben desselben zur Folge haben kann.

Falls in Schritt S1 dagegen festgestellt wird, daß ein bestimmungsgemäßer Einsprung momentan und/oder in absehbarer Zeit danach vorliegt oder vorliegen kann, wird in Schritt S2 die vorstehend bereits erwähnte Modifikation des jeweiligen Datenverarbeitungsprogrammabschnittes und/oder der von diesem benötigten Daten durchgeführt, wodurch diese in einen Zustand übergeführt werden, der einen bestimmungsgemäßen Programmablauf, d. h. ein ordnungsgemäßes Löschen und Überschreiben von Daten des Flash-EPROM ermöglicht.

Die zur genannten Modifikation im einzelnen vorzunehmenden Maßnahmen hängen davon ab, auf welche Weise der jeweilige Datenverarbeitungsprogrammabschnitt und/oder die Daten manipuliert wurden oder weswegen sie in der zum jeweiligen Zeitpunkt vorliegenden Form nicht brauchbar sind.

Unabhängig von der Art und dem Umfang der im Schritt S2 vorzunehmenden Modifikation kann vorgesehen werden, die Ausführung der Modifikation zusätzlich von der Eingabe eines Paßwortes oder dergleichen abhängig zu machen.

Mit der Durchführung des Schrittes S2 ist der betrachtete, in der Fig. 1 veranschaulichte Programmausschnitt abgearbeitet und wird verlassen. Das Ausführen des Schrittes S2 bewirkt, daß ein gegebenenfalls erfolgter oder später noch erfolgender Einsprung in einen Datenverarbeitungsprogrammabschnitt zum Löschen und/oder Überschreiben eines Flash-EPROM tatsächlich ein Löschen und/oder Überschreiben desselben zur Folge haben kann.

Um sicherzustellen, daß das Löschen und/oder Überschreiben von Daten in einem Flash-EPROM bei bestimmungsgemäßem Einsprung in den entsprechenden Datenverarbeitungsprogrammabschnitt tatsächlich auch ausgeführt wird, muß gewährleistet werden, daß eine gegebenenfalls erforderliche Modifikation entsprechend Schritt S2 des in der Fig. 1 gezeigten Programmausschnittes rechtzeitig vor Beginn der Ausführung des betreffenden Datenverarbeitungsprogrammabschnittes oder vor dem Zugriff auf die dann benötigten Daten ausgeführt wird.

Alternativ oder zusätzlich kann der in der Fig. 1 gezeigte Verfahrensabschnitt beispielsweise auch automatisch wiederholt in mehr oder weniger regelmäßigen kurzen Zeitabständen oder gezielt auf das Auftreten gewisser Ereignisse hin ausgeführt werden.

Eine mehrfache oder wiederholte Ausführung des in der Fig. 1 gezeigten Verfahrensabschnittes hat den Vorteil, daß eine gegebenenfalls bereits vorgenommene Modifikation (Schritt S2) bei zwischenzeitlich veränderten Bedingungen wieder rückgängig bzw. unwirksam gemacht werden kann.

Zur Erhöhung der Sicherheit des Schutzmechanismus kann vorgesehen werden, daß die Durchführung der Modifikation (Schritt S2) zusätzlich davon abhängig gemacht wird, daß diese zuvor vom externen Programmiergerät veranlaßt oder wenigstens erlaubt wurde.

Unabhängig davon muß vorzugsweise unmittelbar nach vollendeter Ausführung des Löschens und/oder Überschreibens des Flash-EPROM die in Schritt S2 vorgenommene Modifikation ebenfalls wieder rückgängig bzw. unwirksam gemacht werden. Darüber hinaus ist bei Bedarf auch nach dem Einschalten, Rücksetzen und dergleichen des Steuergerätes dafür zu sorgen, daß dort kein ordnungsgemäß ausführbarer Datenverarbeitungs-

programmabschnitt bzw. eine ordnungsgemäße Ausführbarkeit gestandene Daten in der Variablen-tabelle vorhanden sind.

Abschließend werden nun unter Bezugnahme auf die Fig. 2A bis 2D die Vorgänge bei einem bestimmungsgemäß veranlaßten Löschen eines Flash-EPROM eingehend beschrieben. Es wird dabei nach wie vor von einem wie in der Fig. 3 gezeigten Aufbau ausgegangen.

Fig. 2A veranschaulicht die Aktivitäten des an das Steuergerät 10 angeschlossenen Programmiergerätes 20.

Das Programmiergerät aktiviert irgendwann nach dem Einschalten selbständig oder auf externe Veranlassung hin ein Protokoll (Schritt S10), um mit dem Steuergerät auf eine festgelegte Art und Weise kommunizieren zu können.

Es sei angenommen, daß ein ordnungsgemäßes Löschen und/oder Überschreiben des Flash-EPROM des Steuergerätes einer vorhergehenden Modifizierung der in der Variablen-tabelle bereitgestellten bzw. bereitzustellenden Daten und Adressen für die unlock cycles bedarf.

Dementsprechend veranlaßt das Programmiergerät vor der Ausgabe des Löschbefehls an das Steuergerät das Einschreiben plausibler, d. h. eine Entriegelung des Flash-EPROM ermöglichender Adreß- und Datenwerte in die RAM-Variablen-tabelle des Steuergerätes, d. h. in die im RAM des Steuergerätes untergebrachte Variablen-tabelle (Schritt S11).

Das Einschreiben dieser — gegebenenfalls vom Programmiergerät bereitgestellten — Werte in die RAM-Variablen-tabelle wird, wie später unter Bezugnahme auf Fig. 2B noch genauer beschrieben werden wird, vom Steuergerät selbst durchgeführt; der Schritt S11 ist deshalb "nur" der Anstoß des Modifikationsschrittes S2 in Fig. 1.

Danach, d. h. in Schritt S12 gemäß Fig. 2A wird durch das Programmiergerät das Löschen des Flash-EPROM des Steuergerätes veranlaßt.

Auch das Löschen wird, wie später unter Bezugnahme auf Fig. 2C noch genauer beschrieben werden wird, vom Steuergerät selbst durchgeführt; der Schritt S12 ist lediglich der bestimmungsgemäße Anstoß hierzu.

Das Programm des Programmiergerätes ist mit Schritt S12 noch nicht beendet. Die im Anschluß daran durchgeführten Operationen sind vorliegend jedoch nicht von Interesse.

Es wird nun unter Bezugnahme auf die Fig. 2B die durch Schritt S11 angestoßene Modifikation der Adreß- und Datenwerte für die unlock cycles in der RAM-Variablen-tabelle durch das Steuergerät beschrieben.

Auf die externe Veranlassung durch das Programmiergerät zur Vorbereitung bzw. Herstellung der Bereitschaft des Steuergerätes zum Löschen und/oder Überschreiben des Flash-EPROM (Schritt S11) wird im Steuergerät in Schritt S20 zunächst überprüft, ob überhaupt ein Programmiergerät angeschlossen ist und ob ein Kommunikationsprotokoll aktiviert wurde. Auf diese Weise wird festgestellt, ob die externe Veranlassung, die nur durch eine hierfür vorgesehene Vorrichtung, also ein Programmiergerät oder dergleichen erfolgen darf, tatsächlich auch von einer solchen Vorrichtung ausgeht oder wenigstens ausgehen kann, oder ob die vermeintliche externe Veranlassung und damit auch eine gegebenenfalls bereits erfolgte oder noch folgende Veranlassung des Löschens des Flash-EPROM etwa auf eine Störung oder einem unbefugten Eingriff zurückgehen.

Wird in Schritt S20 festgestellt, daß kein Programmiergerät angeschlossen ist und/oder kein Kommunikationsprotokoll aktiviert ist, wird der in Fig. 2B gezeigte Verfahrensabschnitt verlassen, ohne ein Überschreiben der RAM-Variablentabelle durchzuführen.

Andernfalls, d. h. wenn ein Programmiergerät angeschlossen und ein Kommunikationsprotokoll aktiviert ist, also ein bestimmungsgemäß veranlaßtes Löschen und/oder Überschreiben des Flash-EPROM zu erwarten ist, schreitet der Ablauf zu Schritt S21, wo unmittelbar vor dem Überschreiben der RAM-Variablentabelle sicherheitshalber überprüft wird, ob die Adresse an welche die für die RAM-Variablentabelle bestimmten Adressen- und Datenwerte geschrieben werden sollen, innerhalb der RAM-Variablentabelle liegt.

Wird in Schritt S21 festgestellt, daß die Schreibadresse außerhalb der RAM-Variablentabelle liegt, wird der in Fig. 2B gezeigte Verfahrensabschnitt verlassen, ohne ein Überschreiben der RAM-Variablentabelle durchzuführen.

Andernfalls, d. h. wenn die Schreibadresse innerhalb der RAM-Variablentabelle liegt, schreitet der Ablauf zu Schritt S22, wo das Einschreiben der Adreß- und Datenwerte in die RAM-Variablentabelle erfolgt. Der in der Fig. 2B gezeigte Verfahrensabschnitt ist damit ordnungsgemäß beendet, und das Steuergerät ist auf ein Löschen und/oder Überschreiben des Flash-EPROM vorbereitet.

Es wird nun unter Bezugnahme auf die Fig. 2C das durch Schritt S12 angestoßene Löschen des Flash-EPROM durch das Steuergerät beschrieben.

Auf die externe Veranlassung durch das Programmiergerät zum Löschen und/oder überschreiben des Flash-EPROM durch das Steuergerät (Schritt S12) wird im Steuergerät in Schritt S30 zunächst überprüft, ob überhaupt ein Programmiergerät angeschlossen ist und ob ein Kommunikationsprotokoll aktiviert wurde. Auf diese Weise wird — ähnlich wie bei Schritt S20 in Fig. 2B festgestellt, ob die externe Veranlassung, die nur durch eine hierfür vorgesehene Vorrichtung, also ein Programmiergerät oder dergleichen erfolgen darf, tatsächlich auch von einer solchen Vorrichtung ausgeht oder wenigstens ausgehen kann, oder ob die vermeintliche externe Veranlassung etwa auf eine Störung oder einem unbefugten Eingriff zurückgeht.

Wird in Schritt S20 festgestellt, daß kein Programmiergerät angeschlossen ist und/oder kein Kommunikationsprotokoll aktiviert ist, wird der in Fig. 2C gezeigte Verfahrensabschnitt verlassen, ohne ein Löschen des Flash-EPROM durchzuführen.

Andernfalls, d. h. wenn ein Programmiergerät angeschlossen und ein Kommunikationsprotokoll aktiviert ist, schreitet der Ablauf zu Schritt S31, wo das Löschen des Flash-EPROM erfolgt.

Nach Beendigung des Löschvorganges, also in Schritt S32 gemäß Fig. 2C wird die RAM-Variablentabelle zerstört, d. h. mit Werten versehen, die eine Entriegelung des Flash-EPROM durch die unlock cycles ausschließen.

Der in der Fig. 2C gezeigte Verfahrensabschnitt, d. h. das Löschen des Flash-EPROM ist durch das erneute Sichern des Steuergerätes gegen ein nicht bestimmungsgemäßes Löschen und/oder Überschreiben ordnungsgemäß beendet.

Eine wie in Schritt S32 erfolgende Zerstörung der RAM-Variablentabelle, muß, wie bereits angesprochen, auch nach dem Einschalten, dem Rücksetzen und dergleichen des Steuergerätes durchgeführt werden, um zu verhindern, daß die zu diesem Zeitpunkt in der RAM-

Variablentabelle stehenden Werte zufällig eine Entriegelung des Flash-EPROM ermöglichen. Ein derartiger Vorgang ist in der ohne weitere Erläuterungen verständlichen Fig. 2D dargestellt.

Das unter Bezugnahme auf die Fig. 2A bis 2D beschriebene praktische Beispiel bezog sich auf das Löschen des Flash-EPROM. Entsprechende Vorgänge sollten in entsprechender Weise bei jeglichen Aktionen stattfinden, die eine Speicherinhaltsveränderung des Flash-EPROM bezwecken, also auch beim überschreiben, Umprogrammieren etc.

Auf die beschriebene Weise kann zuverlässig sichergestellt werden, daß ein Löschen und/oder Überschreiben des Flash-EPROM nur dann durchgeführt wird, wenn es bestimmungsgemäß veranlaßt wurde.

Patentansprüche

1. Verfahren zum Betreiben eines Steuergerätes (10) mit einer über eine Programmiervorrichtung (20) programmierbaren Speichereinrichtung (14), wobei das Löschen und das überschreiben des Inhalts der Speichereinrichtung jeweils unter Ausführung eines Datenverarbeitungsprogrammabschnittes und unter Verwendung von Daten durchgeführt wird, dadurch gekennzeichnet, daß wenigstens entweder der Datenverarbeitungsprogrammabschnitt oder die Daten derart bereitgestellt werden, daß sie vor deren Verwendbarkeit zur Herbeiführung eines Löschens oder eines überschreibens einer Modifikation bedürfen, und daß diese Modifikation erst durchgeführt wird, wenn festgestellt wird, daß ein Einsprung in den Datenverarbeitungsprogrammabschnitt bestimmungsgemäß erfolgt ist oder erfolgen wird oder erfolgen kann.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der jeweils bereitgestellte Datenverarbeitungsprogrammabschnitt vor dessen Modifikation derart codiert ist, daß er zumindest teilweise nicht oder nicht ordnungsgemäß ausführbar ist.
3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die besagten Daten durch den jeweiligen Datenverarbeitungsprogrammabschnitt verwendet werden, um zum Lösen der Verriegelung der Speichereinrichtung (14) gegen ein Löschen oder überschreiben des Inhalts der Speichereinrichtung dienende Entriegelungszyklen zu generieren, wozu bestimmte Daten an bestimmte Adressen der Speichereinrichtung ausgegeben werden.
4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die bereitgestellten Daten vor deren Modifikation derartige Werte aufweisen, daß der Datenverarbeitungsprogrammabschnitt nicht in der Lage ist, hieraus zur Entriegelung der Speichereinrichtung (14) geeignete Entriegelungszyklen zu generieren.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß auf einen bestimmungsgemäßen Einsprung in den Datenverarbeitungsprogrammabschnitt geschlossen wird, wenn ermittelt wird, daß Umstände vorliegen, die ein bewußtes und gewolltes Löschen oder überschreiben des Inhalts der Speichereinrichtung (14) wahrscheinlich erscheinen lassen.
6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß auf einen bestimmungsgemäßen Einsprung in den Datenverarbeitungsprogrammab-

schnitt geschlossen wird, wenn ermittelt wird, daß ein externes Programmiergerät (20) am Steuergerät (10) angeschlossen ist.

7. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß auf einen bestimmungsgemäßen Einsprung in den Datenverarbeitungsprogrammabschnitt geschlossen wird, wenn ermittelt wird, daß ein an das Steuergerät (10) angeschlossenes externes Programmiergerät (20) aktiviert ist.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Datenverarbeitungsprogrammabschnitt oder die Daten nach einem erfolgten Löschen oder Überschreiben des Inhalts der Speichereinrichtung (14) und gegebenenfalls auch nach einem Einschalten oder Rücksetzen des Steuergerätes (10) einer derartigen Behandlung unterworfen werden, daß sie ohne erneute Modifikation beim nächsten Einsprung in den Datenverarbeitungsprogrammabschnitt wieder derart bereitgestellt werden, daß sie nicht zur Herbeiführung eines Löschens oder eines Überschreibens der Speichereinrichtung geeignet sind.

Hierzu 6 Seite(n) Zeichnungen

25

30

35

40

45

50

55

60

65

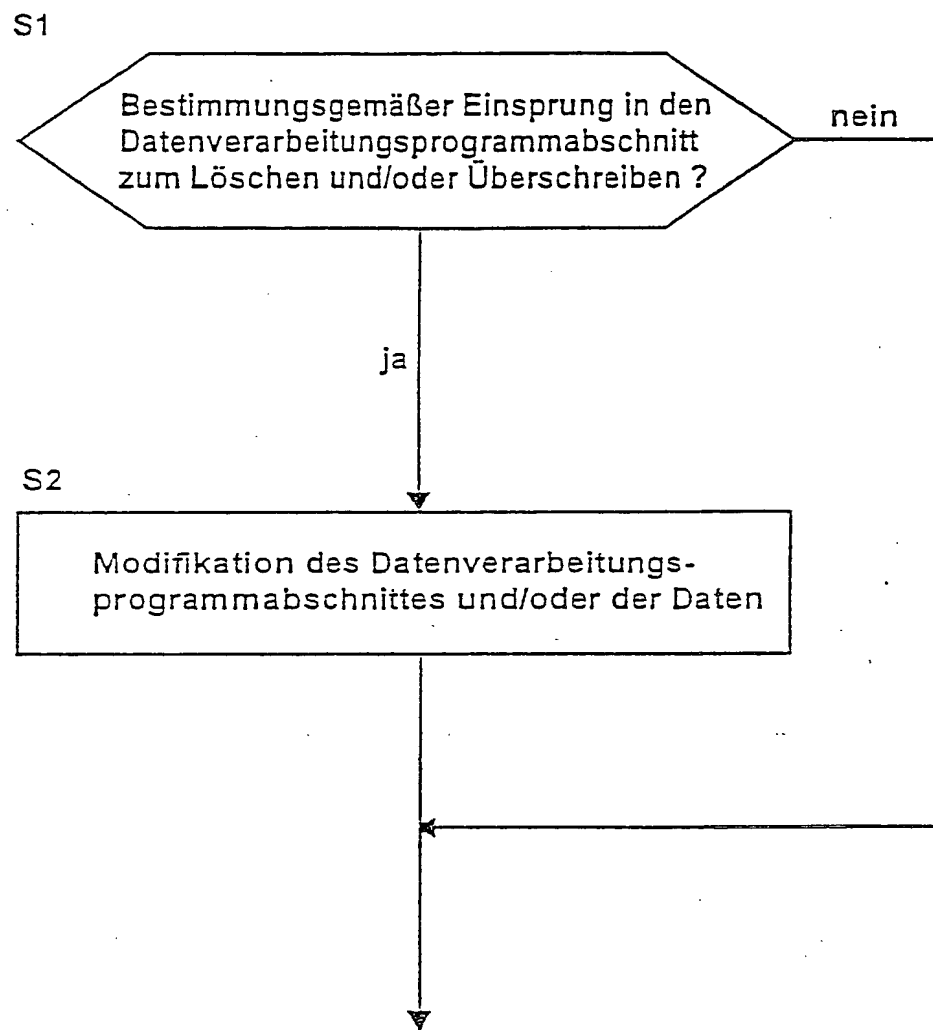


FIG. 1

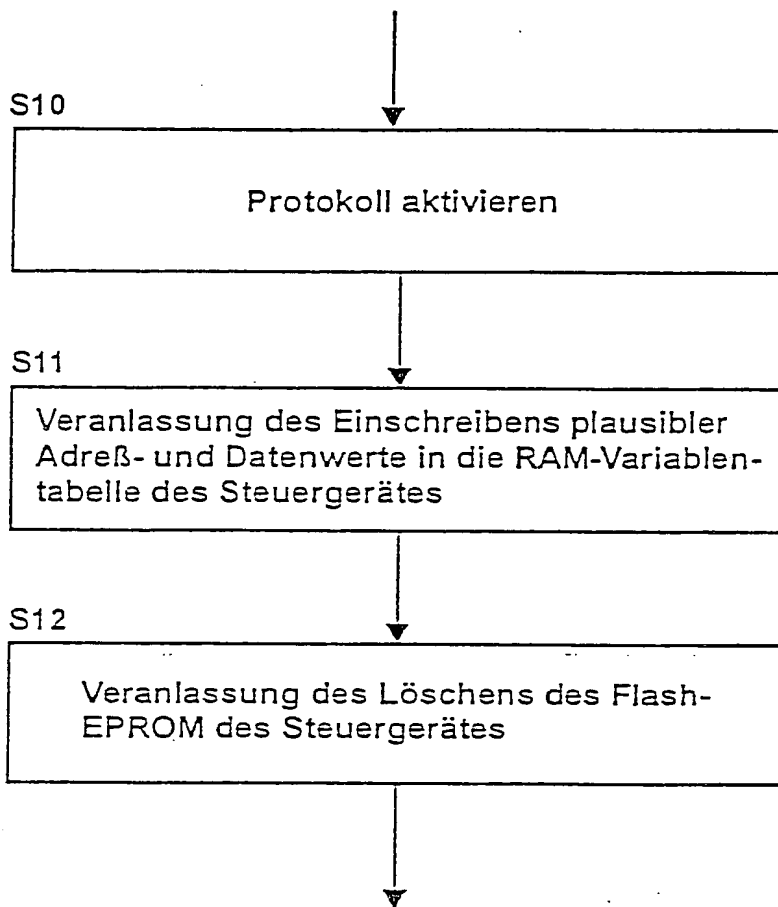


FIG. 2A

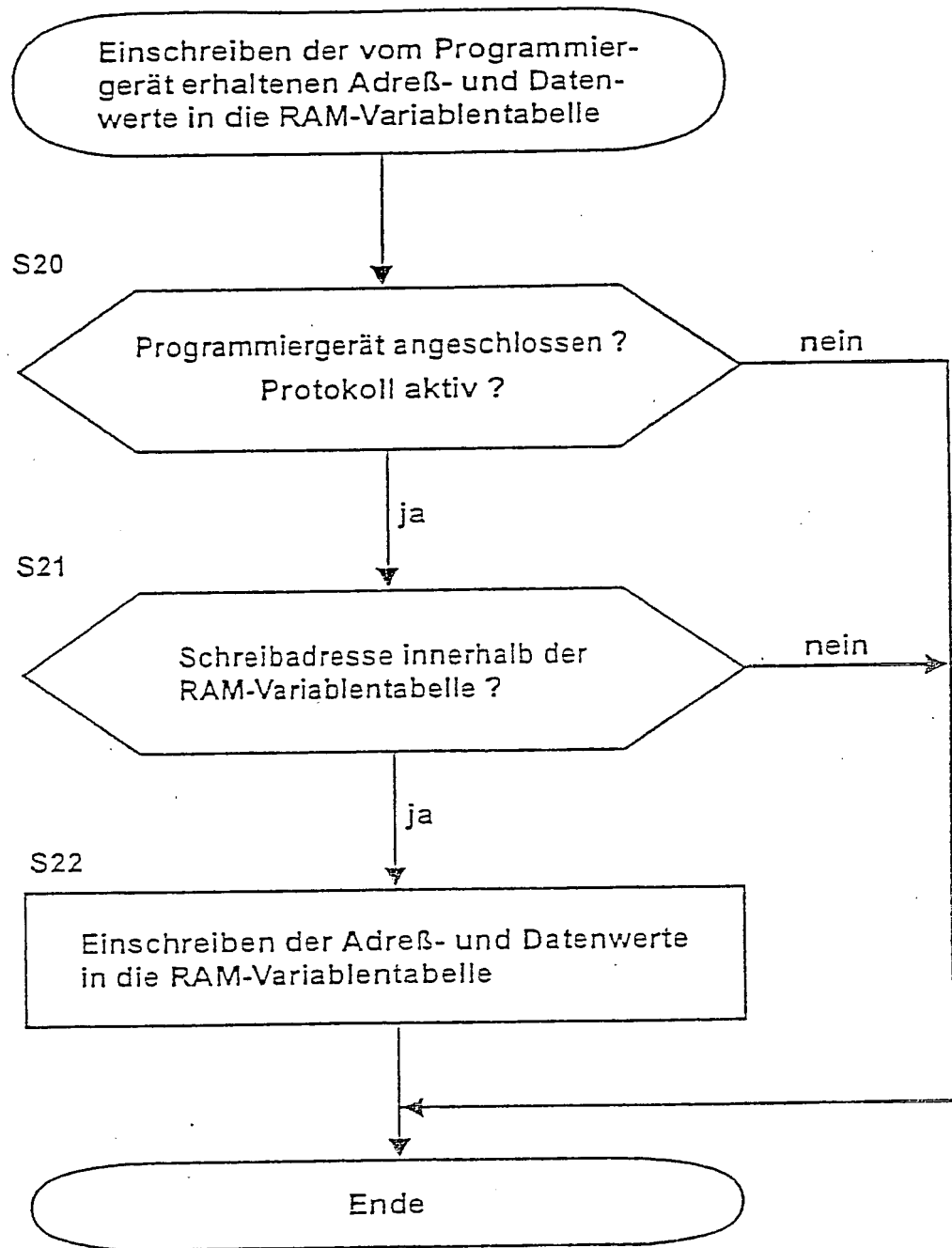


FIG. 2B

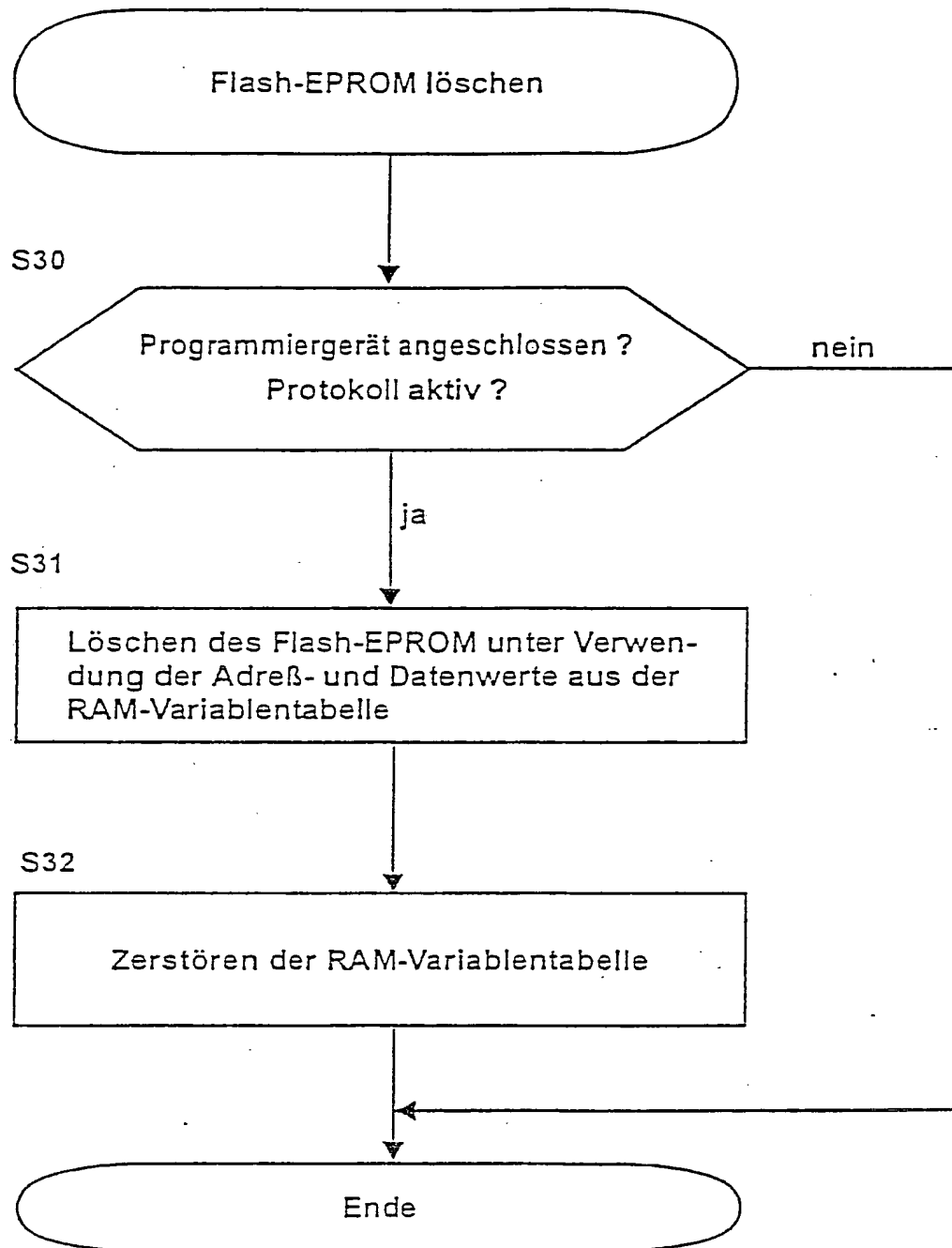


FIG. 2C

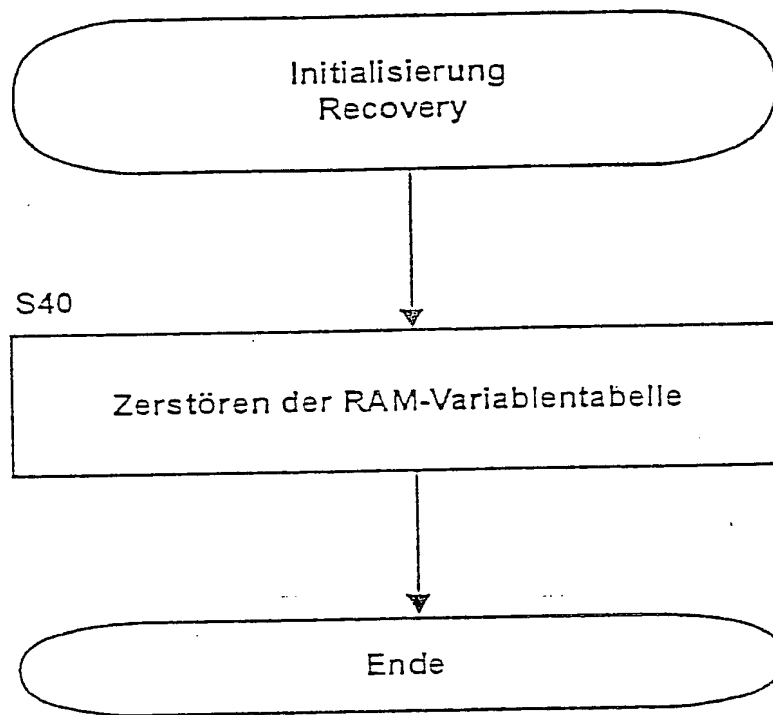


FIG. 2D

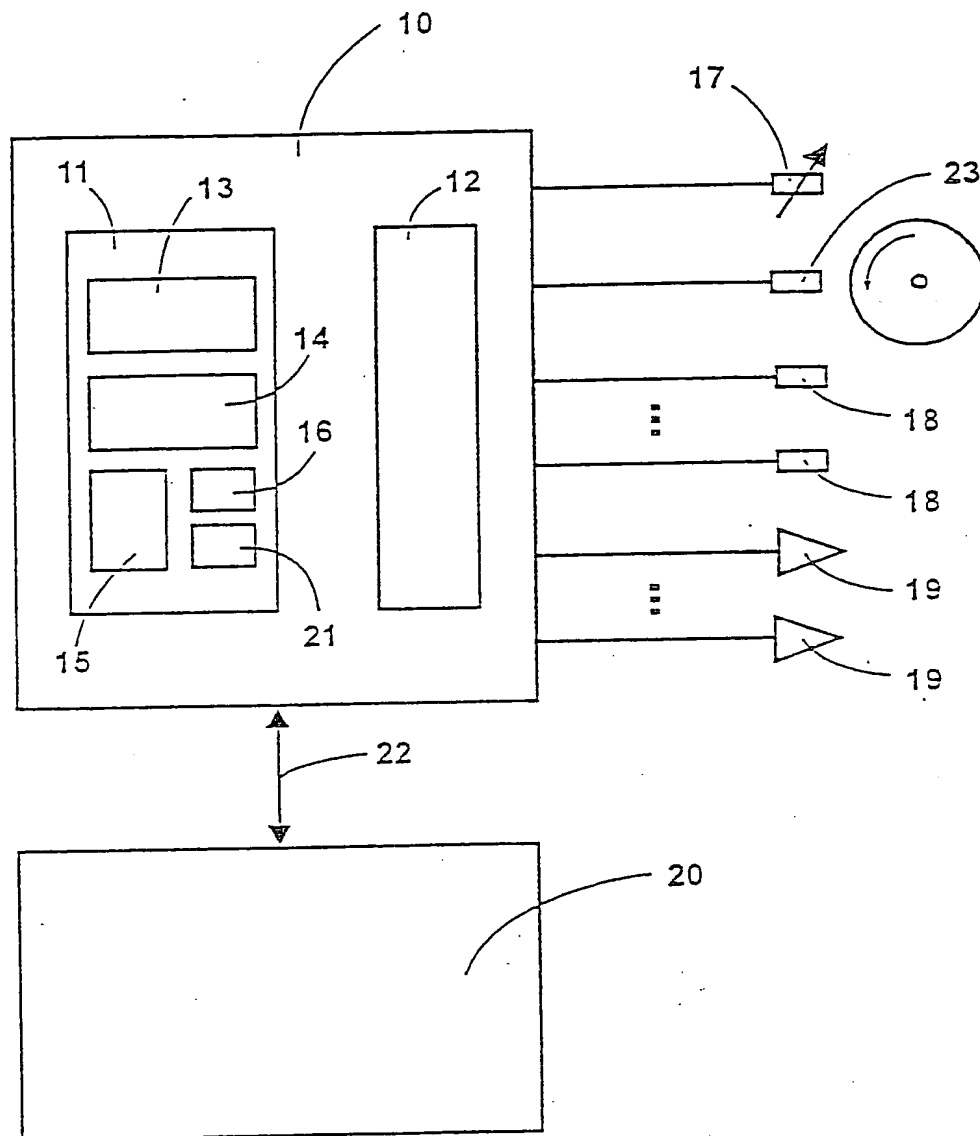


FIG. 3

THIS PAGE BLANK (USPTO)